United Nations ST/SGB/2004/15

Secretariat

29 November 2004

Secretary-General's bulletin

Use of information and communication technology resources and data*

The Secretary-General, for the purposes of defining the proper use of information technology and related resources and data, and of ensuring the security and technical integrity of the system, promulgates the following:

Section 1
Definitions

The following definitions shall apply for the purposes of the present bulletin:

(a) *Authorized user*: any staff member who is authorized to use information and communication technology (ICT) resources;

(b) *ICT resource*: any tangible or intangible asset capable of generating, transmitting, receiving, processing, or representing data in electronic form, where the asset is owned, licensed, operated, managed, or made available by, or otherwise used by, the United Nations;

(c) *ICT data*: any data or information, regardless of its form or medium, which is or has been electronically generated by, transmitted via, received by, processed by, or represented in an ICT resource;

(d) *Official use*: use of ICT resources by an authorized user in the discharge of his or her official functions and within the scope of his or her authorization;

(e) *Personal use*: use of ICT resources by an authorized user for other than official purposes and within the scope of his or her authorization;

* The present bulletin includes a commentary on certain provisions, which is contained in the annex. The commentary is designed to explain such provisions and to help those subject to them to understand them by placing the provisions in context, citing related administrative issuances and providing examples. It is not part of the bulletin and so is not a legal "norm" or imperative, nor does it have the legal force of a rule. It is, however, an official guide published by the Organization for the use of management and staff on the scope and application of the provisions discussed. Those subject to the bulletin may thus safely rely on the commentary to guide their actions since management will use it in interpreting and applying those provisions. The commentary may be updated from time to time in consultation with representatives of the staff in the Staff-Management Coordination Committee established under chapter VIII of the Staff Rules in the light of experience in applying the rules to specific instances.

04-62594 (E) 061204

(f) *Sensitive data*: ICT data that is classified or the use or distribution of which is otherwise restricted pursuant to applicable administrative issuances.

Section 2
Conditions applicable to use of ICT resources and ICT data

(a) Use of ICT resources and ICT data shall in all cases be in accordance with the provisions set out in this bulletin and such other administrative issuances as may apply to them;

(b) Authorized users shall promptly report to the appropriate United Nations authority any violation of the provisions of this bulletin of which they become aware.

Section 3
Official use

3.1 Authorized users shall ensure that their use of ICT resources and ICT data is consistent with their obligations as staff members or such other obligations as may apply to them, as the case may be.

3.2 Authorized users shall use their best efforts:

(a) To ensure the accuracy of any ICT data for which they are responsible;

(b) To preserve and protect ICT resources and ICT data which may be needed by the Organization for any purpose.

3.3 Access to, possession of, or distribution of sensitive data shall be in accordance with all regulations, rules and administrative issuances applicable to such sensitive data.

Section 4
Limited personal use

4.1 Authorized users shall be permitted limited personal use of ICT resources, provided such use:

(a) Is consistent with the highest standard of conduct for international civil servants (among the uses which would clearly not meet this standard are use of ICT resources for purposes of obtaining or distributing pornography, engaging in gambling, or downloading audio or video files to which a staff member is not legally entitled to have access);

(b) Would not reasonably be expected to compromise the interests or the reputation of the Organization;

(c) Involves minimal additional expense to the Organization;

(d) Takes place during personal time or, if during working hours, does not significantly impinge on such working hours;

(e) Does not adversely affect the ability of the authorized user or any other authorized user to perform his or her official functions;

(f) Does not interfere with the activities or operations of the Organization or adversely affect the performance of ICT resources.

4.2 When making personal use of ICT resources, authorized users shall ensure that any such use clearly indicates that it is personal and not official in nature.

4.3 Personal use is a privilege that may be modified or withdrawn at any time, depending on the needs of the Organization. Authorized users shall bear full responsibility and liability in connection with their personal use of ICT resources and the Organization shall not bear any responsibility or liability in respect thereof.

Section 5
Prohibited activities

5.1 Users of ICT resources and ICT data shall not engage in any of the following actions:

(a) Knowingly, or through gross negligence, creating false or misleading ICT data;

(b) Knowingly, or through gross negligence, making ICT resources or ICT data available to persons who have not been authorized to access them;

(c) Knowingly, or through gross negligence, using ICT resources or ICT data in a manner contrary to the rights and obligations of staff members;

(d) Knowingly and without justification or authorization, or through gross negligence, damaging, deleting, deteriorating, altering, extending, concealing, or suppressing ICT resources or ICT data, including connecting or loading any non-ICT resources or ICT data onto any ICT resources or ICT data;

(e) Knowingly accessing, without authorization, ICT data or the whole or any part of an ICT resource, including electromagnetic transmissions;

(f) Knowingly, or through gross negligence, using ICT resources or ICT data in violation of United Nations contracts or other licensing agreements for use of such ICT resources or ICT data or in violation of international copyright law;

(g) Knowingly, or through gross negligence, attempting, aiding or abetting the commission of any of the activities prohibited by this section.

Section 6
Rights in ICT resources; protection of technical integrity and performance of ICT resources

6.1 (a) The Organization shall retain all rights in ICT resources and ICT data and in any work product of an authorized user using ICT resources or ICT data;

(b) The Organization shall have the right to block or restrict access to any ICT resource or ICT data, at any time and without notice, when necessary for maintaining or restoring the technical integrity or performance thereof or for any other appropriate purpose, including prevention of any of the activities prohibited under section 5 of this bulletin.

Section 7
Monitoring and investigations

7.1 All use of ICT resources and ICT data shall be subject to monitoring and investigation as set forth in section 8 and section 9.

7.2 Monitoring and investigations shall be conducted only by the Information Technology Services Division (ITSD), corresponding offices away from Headquarters as designated by the Department of Management, or the Office of Internal Oversight Services (OIOS), in accordance with the procedures set out in section 8 and section 9.

7.3 Officials authorized to monitor or investigate the use of ICT resources shall have access to all ICT resources and ICT data, including data files, word processing files, e-mail messages, LAN records, Intranet/Internet access records, computer hardware and software, telephone services and any other data accessible to or generated by users.

Section 8
Monitoring and investigations conducted by ITSD or corresponding offices away from Headquarters

8.1 Technical monitoring of the use of ICT resources is routinely performed for troubleshooting, diagnostics, statistical analysis and performance tuning. This may include the compiling of aggregated data for a general monitoring of usage.

8.2 At any time there is reason to believe that there has been use which interferes with the operation of ICT resources or technical disruption of ICT resources, ITSD or a corresponding office away from Headquarters may initiate monitoring or an investigation.

8.3 ITSD or the corresponding office away from Headquarters shall conduct an investigation upon request from any official authorized to conduct an investigation under ST/AI/371, or OIOS.

8.4 (a) Except as provided in section 9.1, requests for investigation under ST/AI/371 of the use of ICT resources shall be addressed to the Under-Secretary-General for Management or the Chief of Administration at offices away from Headquarters. Such requests shall be made in writing and provide a brief description of the data required, the name of the staff member or other individual to be investigated and the name of the authorized official from the requesting office to whom the records are to be delivered;

(b) In exceptional cases, an investigation may begin on the basis of a verbal request from an authorized official of the requesting office on the understanding that a written request shall be submitted promptly thereafter;

(c) The investigation shall begin only after the Under-Secretary-General for Management or the Chief of Administration at offices away from Headquarters, as the case may be, has approved the request for investigation;

(d) Except in the event of an emergency, before granting any request to investigate, the Under-Secretary-General for Management or the Chief of Administration at offices away from Headquarters, as the case may be, shall consult with the Chief of Investigations, OIOS, to ensure that the request does not interfere with the mandate and responsibilities of that Office.

8.5 The following procedures shall apply in cases of such investigations:

(a) Staff members and their supervisors shall be informed immediately preceding access to their ICT resources or ICT data, including electronic files, e-mail and Intranet/Internet access records, by the office conducting the investigation;

(b) (i) Whenever practicable, physical investigations involving ICT resources or ICT data shall be performed in the presence of the staff member, his or her supervisor and a representative from the requesting office;

(ii) If necessary to ensure the integrity of the investigation, the staff member may be denied access to the ICT resources and ICT data under investigation, including computers, electronic files and e-mail accounts;

(c) The authorized official of the requesting office shall be required to sign a note confirming receipt of any data retrieved;

(d) A special register shall be maintained in a secure location in ITSD or the corresponding office away from Headquarters undertaking the investigation, recording a brief description of the request for investigation, the requestor's name, the activities undertaken in carrying out the investigation, the name of the personnel performing such activities and the type of information retrieved and provided to the requester;

(e) The data retrieved and provided to the requester shall not be retained by ITSD or the corresponding office away from Headquarters, as the case may be. The original signed written request and receipt for any data provided to the requesting office shall be kept in a separate file in a secure location in the Office of the Under-Secretary-General for Management or in the corresponding office away from Headquarters;

(f) Monitoring or investigation shall continue for only so long as is reasonably necessary to ascertain whether the suspected misconduct has occurred. If no further action will be taken in regard to such suspected violation, the staff member involved shall be so informed by the office that requested such monitoring or investigation to the extent required under ST/AI/371.

Section 9
Investigations by OIOS

9.1 OIOS, in accordance with its mandate, shall initiate and carry out investigations and otherwise discharge its responsibilities without any hindrance or need for prior clearance by any officer of the Organization.

9.2 The following provisions shall apply to investigations carried out by OIOS involving ICT resources or ICT data:

(a) Requests for access to ICT resources or ICT data by OIOS need not be in writing or submitted in advance, where it is not practicable to do so;

(b) OIOS shall have the authority to access all ICT resources and ICT data remotely without informing the staff member;

(c) Physical access to ICT resources located in a staff member's workspace, if practicable, shall be conducted in the presence of the staff member concerned and/or the head of the staff member's division, section or unit;

(d) OIOS shall maintain a written record of its access to any ICT resources or ICT data, recording a brief description of the activities undertaken in carrying out the investigation, the name of the personnel performing such activities and the type of information retrieved; no additional records of such access shall be retained by any other office;

(e) ITSD or the corresponding office away from Headquarters shall designate specific personnel, limited to a specific officer and not more than two alternates, to provide OIOS, upon its request, as it deems necessary or appropriate, with any assistance for obtaining access to ICT resources or ICT data. Different ITSD officers may be designated for different categories of ICT resources.

Section 10
Final provision

The present bulletin shall enter into force on 1 December 2004.

(*Signed*) Kofi A. **Annan**
Secretary-General

Annex to the Secretary-General's bulletin

Commentary

A. Commentary on section 1

1. This section provides definitions for key terms used throughout the bulletin.

2. Definition (a) covers all staff members who are authorized to use ICT resources. This would not include contractors, consultants, gratis personnel, interns, certain United Nations officials who are not staff members and other individuals affiliated with the Organization who are not staff members, but who are authorized to use ICT resources. Accordingly, the agreements or other documents governing the appointment of such individuals or entities should make the terms of this bulletin applicable to them, mutatis mutandis, whether by specific reference to this bulletin or other appropriate means.

The authorization referred to in this definition and throughout the bulletin (except for provision 4 (e)) is that which can be reasonably construed to be granted under the user's official job responsibilities or by instructions from a superior whose official job responsibilities permit the giving of such instructions.

3. Definition (b) is intended to cover all hardware or software capable of handling or storing electronic data. Accordingly, it includes computer hardware (e.g., desktops, laptops, servers, printers), computer software (e.g., operating systems, productivity applications, database management systems), computer networks (e.g., physical media, switching equipment, firewalls, wireless facilities), telephone hardware, software and networks (e.g., wired PBX, cellular telephones), sound systems, voting systems, television and radio facilities, personal digital assistants, including those with wireless web and e-mail capabilities, security equipment (e.g., sensors, cameras, alarms, electronic access doors) and electronic building equipment (e.g., elevators, generators, heating, ventilation and air conditioning).

4. Definition (c) is intended broadly to cover all data or information that is created or received by the United Nations. It includes all data and information, regardless of its origin or the form it may subsequently take (e.g., telephone conversations, telephone logs, information transferred to a memo or other non-electronic medium from e-mail, word processing, IMIS, fax, or other electronic media).

5. In definition (d), "official functions" would include activities reasonably related to staff representation, such as the convocation of meetings, election campaigns for staff unions, committees, associations and joint bodies, and discussion of staff representation business.

6. The authorization referred to in definition (e) is that which is granted by section 4 of this bulletin.

7. Together with the definition of "authorized user", definitions (d) and (e) in section 1 create four categories of individuals: (i) users who are not authorized users; (ii) authorized users engaged in official use; (iii) authorized users engaged in

personal use; and (iv) authorized users engaged in use that is outside their scope of authorization.

8. Definition (f) is intended to cover ICT data which, for reasons of security, safety, privacy, confidentiality or other reasons, is classified or requires special protection, handling and awareness, in accordance with present and future administrative issuances. Regarding current issuances on information that is classified or the distribution of which is otherwise restricted, see ST/SGB/272, ST/AI/326 and ST/AI/189/Add.16.

B. Commentary on section 2

1. In provision 2 (a), other administrative issuances which apply to ICT resources and ICT data include those cited above in reference to the definition of "sensitive data".

2. Provision 2 (b) imposes an obligation on staff members to report violations of the bulletin of which they become aware, even if the violation relates to ICT resources or ICT data that the staff member is not authorized to use or to which the staff member is not authorized to have access. Such a reporting obligation is consistent with obligations imposed by other administrative issuances, for example, ST/SGB/2003/13 regarding sexual exploitation and sexual abuse. However, this provision is intended to cover only violations of which staff members become aware in the normal course of their activities. In accordance with provision 5.1 (c) of this bulletin, staff members may not engage in investigations into the use of ICT resources or ICT data by other staff members without authorization. The appropriate United Nations authority to which violations should be reported may vary depending on the circumstances. Among the authorities to whom it may be appropriate to report violations would be a supervisor, the head of a unit, or OIOS.

C. Commentary on section 3

1. Authorized users are encouraged to make maximum use of ICT resources and ICT data, to the extent of their authorization to do so and with a view to performing their duties as effectively and efficiently as possible.

2. With regard to provision 3.1, authorized users are required to ensure that their use of ICT resources and ICT data are consistent with all other obligations relating thereto. In the case of staff members, this would include the Staff Regulations and Rules and the status, basic rights and duties of United Nations staff members (ST/SGB/2002/13).

3. With regard to provision 3.2, as part of their obligations, authorized users must use their best efforts to make ICT data accessible to any other authorized user who requires such ICT data for the performance of the authorized user's official functions. The obligation to use best efforts to preserve and protect ICT resources and ICT data is especially important where they are required for purposes of conducting an investigation.

D. Commentary on section 4

1. This section recognizes that staff members may from time to time use ICT resources for personal purposes and allows limited use for such purposes subject to certain conditions.

2. Provision 4.1 (a) requires that an authorized user's personal use be consistent with the highest standard of conduct for international civil servants. This standard is elaborated in the Staff Regulations and Rules and the status, basic rights and duties of United Nations staff members (ST/SGB/2002/13).

3. In provision 4.1 (c), minimal additional expense would include use of limited amounts of consumables, such as paper, ink, or toner, general wear and tear on equipment and nominal costs incurred with telecommunications traffic.

4. With regard to provision 4.2, in some cases, the nature or context of the use will clearly indicate that the use is personal and not official. In cases where the non-official nature of the use is not clear, the non-official nature of the use can be indicated, in the case of e-mail messages and other communications, by including the following disclaimer: "This communication is personal, and not official, in nature." The Department of Management may, in consultation with the Office of Legal Affairs, authorize alternative disclaimers for this purpose. Staff members should be careful to keep communications of a personal nature separate from those of an official nature.

5. With regard to provision 4.3, staff members should be aware that personal use of ICT resources, including any communications relating thereto, will not be considered official acts entitled to the Organization's privileges and immunities and that the Organization will cooperate with law enforcement authorities in addressing any personal use of an illegal nature.

E. Commentary on section 5

1. This section enumerates certain activities in which users of ICT resources and ICT data may not engage. In this regard, please see also paragraph 2 of the commentary to section 4.

2. Examples of activities prohibited under provision 5.1 (a) would include the creation of fraudulent documents, the modification of information so as to render it false and the forgery of electronic signatures.

3. An example of the activities prohibited under provision 5.1 (b) would be knowingly, or through gross negligence, revealing passwords to, or otherwise permitting the use by, unauthorized individuals of personal accounts to access ICT resources or ICT data.

4. The rights and obligations of staff members referred to in provision 5.1 (c) would include those elaborated in the Staff Regulations and Rules and the status, basic rights and duties of United Nations staff members (ST/SGB/2002/13).

5. An example of the activities prohibited under provision 5.1 (e) would be unauthorized scanning of ICT resources for security vulnerabilities or other purposes.

6. An example of the activities prohibited under provision 5.1 (f) would be knowingly, or through gross negligence, using pirated software, downloading audio or video files to which a staff member is not legally entitled to have access, or using software for which a valid license has not been obtained.

F. Commentary on sections 7, 8 and 9

1. Sections 7, 8 and 9, which govern monitoring and investigations involving ICT resources or ICT data, are premised on the principle that ICT resources or ICT data are the property of the Organization intended for official use and that any use of them by staff members is subject to the rights of the Organization in such ICT resources or ICT data, including the right to access them without the knowledge or consent of the staff member.

2. Sections 8 and 9 establish two regimes for monitoring and investigation of ICT resources and ICT data — that undertaken by ITSD on behalf of units of the Organization other than OIOS and that undertaken by OIOS.

3. Section 8 sets forth procedures applicable to all monitoring and investigations except those covered by section 9 in the case of OIOS.

4. Provision 7.2 sets forth the offices which are authorized to conduct or assist in monitoring and investigations involving ICT resources or ICT data.

5. Section 8 covers monitoring and investigations conducted by ITSD on its own authority or on behalf of other offices. ITSD and the corresponding offices away from Headquarters may undertake monitoring and investigation on their own authority when there has been interference with or technical disruption of ICT resources or ICT data. They may also undertake to assist other offices in investigations authorized in accordance with ST/AI/371. Investigations involving ICT resources or ICT data shall be made, inter alia, where the requesting office determines that there is reason to believe that misconduct, including violations of the provisions of the present bulletin, have occurred. All investigations involving access to ICT resources or ICT data under section 8 (except those under section 8.2) require the prior approval of the Under-Secretary-General for Management or the Chief Administrative Officer at offices away from Headquarters. Where it is unclear which official is the Chief Administrative Officer for this purpose, the approval shall be sought by the most senior official responsible for the management of ICT resources at the given office.

6. Provision 8.5 sets forth the specific procedures applicable to monitoring and investigations of staff members' use of ICT resources and ICT data and sets forth a number of rights of staff members who are the subject of monitoring or investigation, including the right to be notified in advance that ICT resources or ICT data used by them will be accessed.

G. Commentary on section 9

1. This section sets forth the procedures applicable to OIOS investigations involving ICT resources and ICT data. Consistent with the authority provided to OIOS, these procedures do not accord the same rights in regard to notification to staff members as provided under section 8. Such investigations are to be conducted

in full accordance with the procedures and the rights accorded staff members under all issuances applicable to OIOS investigations, including General Assembly resolution 48/218 B, ST/SGB/273 and the OIOS Investigations Division manual.

2. With regard to provision 9.2, among the conditions and procedures applicable to OIOS investigations are that OIOS need not submit requests for access to ICT resources or ICT data in advance and need not obtain the approval of any official outside OIOS for such access. Provision 9.2 (c) recognizes the authority of OIOS to access a staff member's ICT resources and ICT data remotely without informing the staff member. Notably, where OIOS accesses ICT resources located in a staff member's workspace, such access must be conducted, if practicable, in the presence of the staff member and/or the head of the staff member's division, section or unit.